Generalversammlung

Verteilung: Allgemein
31. Januar 2003

Siebenundfünfzigste Tagung
Tagesordnungspunkt 84 *c*)

Resolution der Generalversammlung

[*auf Grund des Berichts des Zweiten Ausschusses (A/57/529/Add.3)*]

57/239. Schaffung einer globalen Kultur der Cyber-Sicherheit

Die Generalversammlung,

feststellend, dass Regierungen, Wirtschaftsunternehmen, andere Organisationen und individuelle Nutzer immer mehr von Informationstechnologien abhängig sind, wenn es darum geht, wesentliche Güter und Dienstleistungen bereitzustellen, Geschäfte abzuwickeln und Informationen auszutauschen,

in der Erkenntnis, dass mit zunehmender Beteiligung der Länder an der Informationsgesellschaft auch die Notwendigkeit der Cyber-Sicherheit zunimmt,

unter Hinweis auf ihre Resolutionen 55/63 vom 4. Dezember 2000 und 56/121 vom 19. Dezember 2001 betreffend die Schaffung einer Rechtsgrundlage für die Bekämpfung des kriminellen Missbrauchs der Informationstechnologien,

sowie unter Hinweis auf ihre Resolutionen 53/70 vom 4. Dezember 1998, 54/49 vom 1. Dezember 1999, 55/28 vom 20. November 2000, 56/19 vom 29. November 2001 und 57/53 vom 22. November 2002 über Entwicklungen auf dem Gebiet der Informationstechnik und der Telekommunikation im Kontext der internationalen Sicherheit,

sich dessen bewusst, dass wirksame Cyber-Sicherheit nicht nur eine Frage des Vorgehens von Regierungen oder Strafverfolgungsbehörden ist, sondern Prävention erfordert und von der gesamten Gesellschaft unterstützt werden muss,

sich ferner dessen bewusst, dass Technologie allein die Cyber-Sicherheit nicht gewährleisten kann und dass der Planung und Steuerung der Cyber-Sicherheit in der gesamten Gesellschaft ein hoher Stellenwert eingeräumt werden muss,

in der Erkenntnis, dass Regierungen, privatwirtschaftliche Unternehmen, sonstige Organisationen sowie individuelle Besitzer und Nutzer von Informationstechnologien in einer ihrer Rolle angemessenen Weise über die jeweiligen Risiken für die Cyber-Sicherheit sowie über entsprechende Präventivmaßnahmen informiert sein müssen und dass sie Verantwortung für die Sicherheit dieser Informationstechnologien übernehmen und Schritte zu ihrer Verbesserung ergreifen müssen,

sowie in der Erkenntnis, dass die Wirksamkeit der internationalen Zusammenarbeit bei der Bekämpfung des kriminellen Missbrauchs der Informationstechnologien und bei der

Vorauskopie des Deutschen Übersetzungsdienstes, Vereinte Nationen, New York. Der endgültige amtliche Wortlaut der Übersetzung erscheint im Offiziellen Protokoll der Generalversammlung bzw. des Sicherheitsrats.

Schaffung einer globalen Kultur der Cyber-Sicherheit durch Lücken beim Zugang der Staaten zu den Informationstechnologien und bei ihrer Nutzung herabgesetzt werden kann, und feststellend, dass der Transfer von Informationstechnologien, insbesondere in die Entwicklungsländer, erleichtert werden muss,

ferner in der Erkenntnis, wie wichtig die internationale Zusammenarbeit für die Herbeiführung der Cyber-Sicherheit ist, in deren Rahmen die einzelstaatlichen Anstrengungen zur Steigerung der personellen Kapazitäten und der Lern- und Beschäftigungsmöglichkeiten, zur Verbesserung der öffentlichen Dienstleistungen und zur Steigerung der Lebensqualität durch den Einsatz hochentwickelter, zuverlässiger und sicherer Informations- und Kommunikationstechnologien und -netzwerke und die Förderung des allgemeinen Zugangs unterstützt werden,

feststellend, dass die Informationssysteme und -netze heute auf Grund der zunehmenden Vernetzung einer größeren Zahl und Vielfalt von Bedrohungen ausgesetzt sind und mehr Angriffsflächen bieten, wodurch neue Sicherheitsprobleme für alle entstehen,

sowie feststellend, dass die zuständigen internationalen und regionalen Organisationen darauf hinarbeiten, die Cyber-Sicherheit und die Sicherheit der Informationstechnologien zu erhöhen,

1. *nimmt Kenntnis* von den in der Anlage zu dieser Resolution enthaltenen Bausteinen, durch die eine globale Kultur der Cyber-Sicherheit geschaffen werden soll;

2. *bittet* alle zuständigen internationalen Organisationen, bei allen künftigen Tätigkeiten auf dem Gebiet der Cyber-Sicherheit unter anderem diese Bausteine zur Schaffung einer derartigen Kultur zu prüfen;

3. *bittet* die Mitgliedstaaten, diese Bausteine unter anderem bei ihren Bemühungen zu berücksichtigen, überall in ihren Gesellschaften eine Kultur der Cyber-Sicherheit für die Anwendung und den Einsatz der Informationstechnologien zu schaffen;

4. *bittet* die Mitgliedstaaten und alle zuständigen internationalen Organisationen, bei ihren Vorbereitungen für den Weltgipfel über die Informationsgesellschaft, der vom 10. bis 12. Dezember 2003 in Genf und im Jahr 2005 in Tunis stattfinden soll, unter anderem diese Bausteine sowie die Notwendigkeit einer globalen Kultur der Cyber-Sicherheit in Betracht zu ziehen;

5. *betont*, dass es geboten ist, den Transfer der Informationstechnologien in die Entwicklungsländer und den Aufbau entsprechender Kapazitäten zu erleichtern, um diesen Ländern bei der Ergreifung von Maßnahmen der Cyber-Sicherheit behilflich zu sein.

78. Plenarsitzung
20. Dezember 2002

Anlage

Bausteine zur Schaffung einer globalen Kultur der Cyber-Sicherheit

Die raschen Fortschritte in der Informationstechnologie haben für Regierungen, privatwirtschaftliche Unternehmen, sonstige Organisationen sowie individuelle Nutzer, die Informationssysteme und -netze entwickeln, besitzen, bereitstellen, steuern, betreuen und nutzen ("die Teilnehmer"), den Umgang mit der Cyber-Sicherheit verändert. Eine globale Kultur der Cyber-Sicherheit erfordert von allen Teilnehmern die Beachtung der folgenden neun einander ergänzenden Bausteine:

a) *Problembewusstsein*. Die Teilnehmer sollten sich darüber im Klaren sein, dass die Sicherheit der Informationssysteme und -netze gewährleistet sein muss, und wissen, was sie tun können, um die Sicherheit zu erhöhen;

b) *Verantwortungsbewusstsein*. Die Teilnehmer sind für die Sicherheit der Informationssysteme und -netze in einer ihrer individuellen Rolle angemessenen Weise verantwortlich. Sie sollten ihre jeweiligen Politiken, Praktiken, Maßnahmen und Verfahren regelmäßig überprüfen und sie daraufhin bewerten, ob sie für ihr Umfeld angemessen sind;

c) *Antwortmaßnahmen*. Die Teilnehmer sollten frühzeitig und kooperativ handeln, um Sicherheitsprobleme zu verhüten, aufzudecken und darauf zu reagieren. Sie sollten nach Bedarf Informationen über Bedrohungen und Schwachstellen austauschen und Verfahren für eine rasche und wirksame Zusammenarbeit anwenden, um Sicherheitsprobleme zu verhüten, aufzudecken und darauf zu reagieren. Dies kann auch einen grenzüberschreitenden Informationsaustausch und eine entsprechende Zusammenarbeit umfassen;

d) *Ethische Fragen*. Angesichts der Allgegenwart der Informationssysteme und -netze in modernen Gesellschaften müssen die Teilnehmer die legitimen Interessen Dritter achten und anerkennen, dass ihr Handeln oder Unterlassen Dritten Schaden zufügen kann;

e) *Demokratie*. Sicherheitsmaßnahmen sollten in Übereinstimmung mit den anerkannten Werten demokratischer Gesellschaften durchgeführt werden, namentlich mit der Freiheit, Gedanken und Ideen auszutauschen, dem freien Informationsfluss, der Vertraulichkeit von Information und Kommunikation, dem angemessenen Schutz persönlicher Informationen, der Offenheit und der Transparenz;

f) *Risikobewertung*. Alle Teilnehmer sollten regelmäßig Risikobewertungen zur Ermittlung von Bedrohungen und Schwachstellen durchführen, die so breit angelegt sind, dass sie wichtige interne und externe Faktoren umfassen, darunter Technologie, physische und menschliche Faktoren, Politiken und Dienstleistungen Dritter, die sich auf die Sicherheit auswirken, die die Festlegung einer annehmbaren Risikoschwelle ermöglichen und die bei der Auswahl geeigneter Kontrollmaßnahmen helfen, um das Risiko einer potenziellen Schädigung der Informationssysteme und -netze gegen die Art und Wichtigkeit der zu schützenden Informationen abzuwägen;

g) *Gestaltung und Durchführung von Sicherheitsmaßnahmen*. Die Teilnehmer sollten die Sicherheit als wesentliches Element in die Planung und Ausgestaltung, den Betrieb und die Nutzung der Informationssysteme und -netze aufnehmen;

h) *Sicherheitsmanagement*. Die Teilnehmer sollten ein umfassendes Sicherheitsmanagementkonzept übernehmen, das auf einer dynamischen, alle Tätigkeitsebenen der Teilnehmer und alle Aspekte ihrer Operationen umfassenden Risikobewertung beruht;

i) *Neubewertung*. Die Teilnehmer sollten die Sicherheit der Informationssysteme und -netze überprüfen und neu bewerten und entsprechende Veränderungen an den Politiken, Praktiken, Maßnahmen und Verfahren auf dem Gebiet der Sicherheit vornehmen, wozu auch das Eingehen auf neue und sich verändernde Bedrohungen und Schwachstellen gehört.